

**Hardware Architecture, Operating System And Network Transport Neutral System, Method And
Computer Program Product For Secure Communications And Messaging
(A-70553/RMA)**

5 WE CLAIM:

1. A hardware architecture, operating system, and network transport neutral method secure communications, the method comprising:

an authorization procedure for authorizing any particular user the right to access a specific resource;

10 a digital certificate procedure that enables at least encryption and digital signatures having lower storage and bandwidth requirements than conventional digital certificates;

a security protocol implementation procedure for implementing two or more security protocols using a common set of data formats, algorithms, subroutines, and procedures;

a secure session interaction procedure having reduced software/firmware computer code/instructions and reduced network bandwidth than conventional secure session interaction procedures;

15 a secure unidirectional messaging procedure using less software/firmware code and reduced network bandwidth than conventional unidirectional messaging procedures;

a secure certificate issuing procedure using less software/firmware code and reduced network bandwidth than conventional secure certificate issuing procedures;

20 a secure response session procedure using less software/firmware code and reduced network bandwidth than conventional secure response procedures; and

a secure unidirectional response messaging procedure using less software/firmware code and reduced network bandwidth than conventional secure unidirectional messaging procedures.

2. A system for secure communications comprising:

25 an authorization module for authorizing any particular user the right to access a specific resource;

a digital certificate encryption module that enables at least encryption and digital signatures having lower storage and bandwidth requirements than conventional digital certificates;

a security protocol module for implementing two or more security protocols using a common set of data formats, algorithms, subroutines, and procedures;

30 a secure session interaction module having reduced software/firmware computer code/instructions and reduced network bandwidth than conventional secure session interaction procedures;

a secure unidirectional messaging module using less software/firmware code and reduced network bandwidth than conventional unidirectional messaging procedures;

35 a secure certificate issuing module using less software/firmware code and reduced network bandwidth than conventional secure certificate issuing procedures;

a secure response session module using less software/firmware code and reduced network bandwidth than conventional secure response procedures; and

a secure unidirectional response messaging module using less software/firmware code and reduced network bandwidth than conventional secure unidirectional messaging procedures.

3. A computer program product for use in conjunction with a computer system having a server and a client, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism, comprising: a program module that directs the computer system and/or components thereof including at least one or the client or server, to function in a specified manner to provide message communications, the message communications occurring in a computer system hardware architecture neutral and operating system neutral and network transport protocol neutral manner for secure communications, the program module including instructions for:

- an authorization procedure for authorizing any particular user the right to access a specific resource;
- a digital certificate procedure that enables at least encryption and digital signatures having lower storage and bandwidth requirements than conventional digital certificates;
- 15 a security protocol implementation procedure for implementing two or more security protocols using a common set of data formats, algorithms, subroutines, and procedures;
- a secure session interaction procedure having reduced software/firmware computer code/instructions and reduced network bandwidth than conventional secure session interaction procedures;
- a secure unidirectional messaging procedure using less software/firmware code and reduced network bandwidth than conventional unidirectional messaging procedures;
- 20 a secure certificate issuing procedure using less software/firmware code and reduced network bandwidth than conventional secure certificate issuing procedures;
- a secure response session procedure using less software/firmware code and reduced network bandwidth than conventional secure response procedures; and
- 25 a secure unidirectional response messaging procedure using less software/firmware code and reduced network bandwidth than conventional secure unidirectional messaging procedures.

4. A hardware architecture, operating system, and network transport neutral method secure communications, said method comprising:
- 30 an authorization procedure for authorizing any particular user the right to access a resource;
 - a digital certification procedure for encryption and digital signing;
 - a security protocol procedure for implementing a plurality of security protocols using a single common set of policies and parameters;
 - a secure session interaction procedure;
 - 35 a secure unidirectional messaging procedure;
 - a secure certificate issuing procedure;
 - a secure response session procedure; and
 - a secure unidirectional response messaging procedure;

said procedures using less software/firmware/computer code and reduced network bandwidth than conventional procedures to accomplish analogous functionality.

2025 RELEASE UNDER E.O. 14176